



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/827,218	04/19/2004	Wael M. Ibrahim	200314912-1	2929

22879 7590 07/18/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

REZA, MOHAMMAD W

ART UNIT	PAPER NUMBER
----------	--------------

2136

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

07/18/2008

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

DETAILED ACTION

1. This is in response to the arguments filed on 05/05/2008.
2. Claims 1-47 are pending in the application.

Response to Amendment

3. The examiner approves election of claims 1-18, and 45-46.

Response to Arguments

4. Applicant's election with traverse of Invention Species I in the reply filed on 09/10/2007 is acknowledged. The traversal is on the ground(s) that applicant argues in general without pointing out the lack of previous restriction requirement that is required by MPEP 808.02. Applicant arguments fail to identify why the inventions I-VII are not related as subcombinations disclosed as usable together in a single combination. This is not found persuasive because examiner could not understand why these different groups of inventions should be considered in one group while distinctly showing the different classes and sub-classes embodied with the claims limitations of the species. These independent and distinct species are required different field of search which is serious burden for examiner. **So, the requirement is still deemed proper and is therefore made FINAL.**

Examiner reviewed the MPEP and found the following part in favor of the species restriction. For purposes of the initial requirement, a serious burden on the examiner may be prima facie shown by appropriate explanation of separate classification, or separate status in the art, or a different field of search as defined in MPEP § 808.02.

808.02 [R-5] Establishing Burden

Where, as disclosed in the application, the several inventions claimed are related, and such related inventions are not patentably distinct as claimed, restriction under 35 U.S.C. 121 is never proper (MPEP § 806.05). If applicant voluntarily files claims to such related inventions in different applications, double patenting may be held. Where the inventions as claimed are shown to be independent or distinct under the criteria of MPEP § 806.05(c) - § 806.06, the examiner, in order to establish reasons for insisting upon restriction, must explain why there would be a serious burden on the examiner if restriction is not required. Thus the examiner must show by appropriate explanation one of the following:

(A) **Separate classification thereof** : This shows that each invention has attained recognition in the art as a separate subject for inventive effort, and also a separate field of search. Patents need not be cited to show separate classification.

(B) **A separate status in the art when they are classifiable together** : Even though they are classified together, each invention can be shown to have formed a separate subject for inventive effort when the examiner can show a recognition of separate inventive effort by inventors. Separate status in the art may be shown by citing patents which are evidence of such separate status, and also of a separate field of search.

(C) **A different field of search** : Where it is necessary to search for one of the inventions in a manner that is not likely to result in finding art pertinent to the other invention(s) (e.g., searching different classes /subclasses or electronic resources, or employing different search queries, a different field of search is shown, even though

the two are classified together. The indicated different field of search must in fact be pertinent to the type of subject matter covered by the claims. Patents need not be cited to show different fields of search.

808.01(a) [R-5] Species

Where there is no disclosure of a relationship between species (see MPEP § 806.04(b)), they are independent inventions. A requirement for restriction is permissible if there is a patentable difference between the species as claimed and there would be a serious burden on the examiner if restriction is not required. See MPEP § 803 and § 808.02. Where there is a relationship disclosed between species, such disclosed relation must be discussed and reasons advanced leading to the conclusion that the disclosed relation does not prevent restriction, in order to establish the propriety of restriction.

806.04(f) [R-3] Restriction Between Mutually Exclusive Species

Where two or more species are claimed, a requirement for restriction to a single species may be proper if the species are mutually exclusive. Claims to different species are mutually exclusive if one claim recites limitations disclosed for a first species but not a second, while a second claim recites limitations disclosed only for the second species and not the first. This may also be expressed by saying that to require restriction between claims limited to species, the claims must not overlap in scope.

As examiner mentioned in the previous office action that how all these four species are grouped in different independent and distinct inventions. Species I are presented a system of cryptographic key maintenance interfacing with for trusted platform which is classified as class

380, subclass 276. Species II are dealing with key storage and prevent performance of an authentication process which is classified as class 713, subclass 155. Species II should be independent and distinct invention by its own class, and subclass because it also includes some other limitations such as key storage hierarchy, executing a first set of processor executable instructions associated with the logic and processor readable data associated with the logic while preventing another logic from reading. In the same way, Species III are drawn to a system using memory for storing the root key, restore the logic, and interfacing the action platform which is classified as class 380, and subclass 264. This group is also independent and distinct from the previous two groups. Species VI are drawn for to a method for validating the trusted platform classified as class 380, and subclass 44. This last group is also independent and distinct as it dealing with establishing an operable connection between the subordinate trusted platform and a trusted platform associated with a key hierarchy, controlling the subordinated trusted platform to be reconfigured to indicate that the subordinate trusted platform performed a requested maintenance, and disestablishing the operable connection between the subordinate trusted platform. So, it is a serious burden for examiner to search this vast field to cover all theses four different species groups with their limitations. As a result, examiner respectfully acknowledges to the applicant that the restriction requirement is still deemed proper and final.

Election/Restriction

5. Restriction to one of the following inventions is required under 35 U.S.C. 121:

- I. Claims 1-18, and 45-46, drawn to a system of cryptographic key maintenance for trusted platform, classified in class 380, subclass 276.

- II. Claims 19, and 41, drawn to a system using the key storage and prevent performance of an authentication process, classified in class 713, subclass 155.
- III. Claims 20-24, and 44, drawn to a system using memory for storing the root key, restore the logic, and interfacing the action of platform, classified in class 380, subclass 262.
- IV. Claims 25-28, and 47, drawn to a system using the platform for backing up the stored key, classified in class 380, subclass 264.
- V. Claims 29-31, and 42, drawn to a system for storing the root key, and copying the root key, classified in class 380, subclass 228.
- VI. Claims 32-37, drawn to a method using key hierarchy, and controlling the subordinated platform, classified in class 380, subclass 44.
- VII. Claims 38-40, and 43, drawn to a method for validating the trusted platform, classified in class 726, subclass 4.

The inventions are distinct, each from the other because of the following reasons:

6. Inventions I-VII are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination is separately usable. Each subcombination has specific limitations and utilities that are not found in the other inventions. See MPEP § 806.05(d).

The examiner has required restriction between subcombinations usable together.

Where applicant elects a subcombination and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all the limitations of the

allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

7. Because these inventions are independent or distinct for the reasons given above and there would be a serious burden on the examiner if restriction is not required because the inventions have acquired a separate status in the art in view of their different classification, restriction for examination purposes as indicated is proper.

8. Because these inventions are independent or distinct for the reasons given above and there would be a serious burden on the examiner if restriction is not required because the inventions require a different field of search (see MPEP § 808.02), restriction for examination purposes as indicated is proper.

9. Because these inventions are independent or distinct for the reasons given above and there would be a serious burden on the examiner if restriction is not required because the inventions have acquired a separate status in the art due to their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

10. Applicant is advised that the reply to this requirement to be complete must include (i) an election of a species or invention to be examined even though the

requirement be traversed (37 CFR 1.143) and (ii) identification of the claims encompassing the elected invention.

The election of an invention or species may be made with or without traverse. To reserve a right to petition, the election must be made with traverse. If the reply does not distinctly and specifically point out supposed errors in the restriction requirement, the election shall be treated as an election without traverse.

Should applicant traverse on the ground that the inventions or species are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the inventions or species to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C.103(a) of the other invention.

11. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

12. **Applicant is reminded that examiner would withheld any further examination of the dependent claims which classified as different species of class and subclass. However, upon allowance of the independent claim those dependent claims will be rejoined with their actual independent claim.** Upon the allowance of a generic claim. Applicant will be entitled to consideration of claims to additional species which depend from or otherwise require all the

limitations of an allowance generic claims as provided by 37 C.F.R. 1.141. If claims are added after the election, applicant must indicate which are readable upon the elected species, MPEP 809.02 (a).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claims 1, 4-5, 7-18, and 45-46 are rejected under 35 U.S.C. 102(e) as being anticipated by Challenger (US patent 7281010).

14. As per claim 1, Challenger discloses a system, comprising: a logic configured to perform one or more of, cryptographic key maintenance, and cryptographic key migration for a trusted platform to which the logic may be bound in a one-to-one manner; and an interface configured to facilitate operably connecting the system to the trusted platform (col. 3, lines 14-46, col. 4, lines 23-45).

15. As per claim 4, Challenger discloses the system where the logic comprises a microprocessor operably connected to a non-volatile memory (col. 3, lines 14-35).

17. As per claim 5, Challenger discloses the system where the logic and the interface comprise part of a USB token (col. 4, lines 5-22).

16. As per claim 7, Challenger discloses the system where performing cryptographic key maintenance includes cloning the trusted platform with the cooperation of a

manufacturer of the trusted platform and an owner of the trusted platform (col. 5, lines 4-18).

17. As per claim 8, Challenger discloses the system where performing cryptographic key maintenance includes having the manufacturer of the trusted platform act as an intermediary and migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform (col. 3, lines 47-67).

18. As per claim 9, Challenger discloses the system where performing cryptographic key migration includes logically attaching a trusted platform module migratable key data structure associated with a first protected storage tree to a second protected storage tree (col. 1, lines 50-67).

19. As per claim 10, Challenger discloses the system where the logic is configured to stow one or more of, a copy of a storage root key, a binding data that facilitates binding the logic to the trusted platform in a one-to-one binding, a processor executable set of instructions that facilitate the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module (col. 3, lines 14-46, col. 4, lines 23-45), and a processor readable set of data that facilitates the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module (col. 1, lines 50-67).

20. As per claim 11, Challenger discloses the system where the logic is configured to facilitate substantially instantaneously restoring a trusted platform module (col. 3, lines 14-46, col. 4, lines 23-45).

21. As per claim 12, Challenger discloses the system where the logic is configured to decrypt One or more of, a key, and a piece of data encrypted by a trusted platform module (col. 4, lines 58-67).

22. As per claim 13, Challenger discloses the system where the logic is configured to execute processor executable instructions associated with the logic while preventing execution of processor executable instructions not associated with the logic (col. 5, lines 33-47).

23. As per claim 14, Challenger discloses the system where the logic is configured to read processor readable data associated with the logic while preventing a second logic from reading the processor readable data associated with the logic (col. 5, lines 4-18).

24. As per claim 15, Challenger discloses the system where the logic is configured to detect whether there is a functional trusted platform module associated with the trusted platform (col. 3, lines 14-46, col. 4, lines 23-45).

25. As per claim 16, Challenger discloses the system where the logic is configured to prevent creation of a new cryptographic key by the system and to prevent performance of an attestation service by the logic (col. 1, lines 50-67).

26. As per claim 17, Challenger discloses the system where binding the logic to the trusted platform in a one-to-one manner includes producing an optimal asymmetric encryption padding (OEAP) binary large object to facilitate copying a storage root key stored in a trusted platform module associated with the trusted platform (col. 3, lines 47-67).

27. As per claim 18, Challenger discloses the system where the logic is configured to

Art Unit: 2136

perform a finite number of cryptographic key maintenance or migration operations (col. 4, lines 58-67).

28. As per claim 45, Challenger discloses a system, comprising: an electronic apparatus configured with a trusted platform module; and an interface operably connected to the electronic apparatus, the interface configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus (col. 3, lines 14-46, col. 4, lines 23-45).

29. As per claim 46, Challenger discloses the system, where the electronic apparatus comprises, one of, a computer, a printer, a cellular telephone, and a digital camera (col. 1, lines 50-67).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

30. Claims 2, 3, 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challenger (US patent 7281010) in view of Ranganathan (US Patent Publication 20050138423).

31. As per claim 2, Challenger discloses the system of the cryptographic key maintenance and the cryptographic key migration (col. 3, lines 14-46, col. 4, lines 23-45). Although, Challenger discloses trusted platform, he does not explicitly disclose performed by the logic comply with the Trusted Computing Group (TCG) specification version 1.1b. However, in the same foeld of endeavor, Ranganathan discloses performed by the logic comply with the Trusted Computing Group (TCG) specification version 1.1b. (paragraph 0042).

Accordingly, it would been obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Ranganathan's teachings of trusted computing group with the teachings of Challenger, for the purpose of suitably using the specific computing group of the trusted platform (paragraph 0042).

32. As per claim 3, Challenger does not disclose the system where the logic comprises an application specific integrated circuit (ASIC). However, Ranganathan discloses where the logic comprises an application specific integrated circuit (ASIC) (paragraph 0033).

The same motivation that was utilized in the combination of claim 2 applies equally as well to claim 3.

33. As per claim 6, Challenger discloses the system wherein an Industrial Standard Architecture interface, an Extended industrial Standard Architecture interface, a wireless connection, and a microchannel interface (col. 5, lines 54-67, col. 6, lines 1-10). He does not expressly discloses where the interface is configured to facilitate oPerably connecting the system to the trusted platform by one or more of, a Universal Serial Bus

Art Unit: 2136

interface, a Small Computer Systems Interface interface, a Peripheral Component Interconnect interface, a PCI Express (PCIE) interface, a 1394 interface. However, Ranganathan discloses where the interface is configured to facilitate operably connecting the system to the trusted platform by one or more of, a Universal Serial Bus interface, a Small Computer Systems Interface interface, a Peripheral Component Interconnect interface, a PCI Express (PCIE) interface, a 1394 interface (paragraphs, 0027-0028).

The same motivation that was utilized in the combination of claim 2 applies equally as well to claim 6.

Conclusion

34. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

Art Unit: 2136

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Nasser G Moazzami/

Mohammad Wasim Reza

Supervisory Patent Examiner, Art Unit 2136

AU 2136